***LISTING OF CLAIMS***

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("~~---~~"), as is applicable:

1. (Currently Amended) An email system for providing email service to a user, comprising:

a computer device of the user configured with a plurality of detection mechanisms that detect undesired email messages that have been received by the user from an email server; and

a user interface installed on the computer device and configured to visually represent that a particular undesired email message was detected using a particular detection mechanism, wherein each of the detection mechanisms is represented using a different visual representation and the user interface upon detecting a drag and drop operation to move an email message from an inbox to a designated folder where the undesired email messages are stored prompts for the moved email message to be marked as a type of undesired email message that is associated with one of the detection mechanisms.

2. (Original) The system of claim 1, wherein the plurality of detection mechanisms includes a mechanism that refuses to detect an email message if the sender of the email message is on a list of senders authorized by the user.

3. (Original) The system of claim 1, wherein the plurality of detection mechanisms includes a mechanism that detects an email message if the sender of the email message is on a list of unauthorized senders.

4. (Original) The system of claim 1, wherein the plurality of detection mechanisms includes a mechanism that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content strings.

5. (Original) The system of claim 1, wherein the plurality of detection mechanisms include a mechanism that is configured to:

analyze the overall content of previous email messages that have been detected; and

detect an email message if the content of the message is similar to the overall content of the previous messages.

6. (Original) The system of claim 1, wherein the plurality of detection mechanisms include:

a first detection mechanism that detects an email message if the sender of the email message is not on a list of senders authorized by the user;

a second detection mechanism that detects an email message if the sender of the email message is on a list of unauthorized senders;

a third detection mechanism that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content string; and

a fourth detection mechanism that is configured to:

analyze the overall content of previous email messages that have been detected;

compare the content of an email message to the overall content and assign a score reflective of a level of similarity for the email message; and

detect the email message if the score is higher than a designated score.

7. (Original) The system of claim 1, wherein the particular undesired email message is, within an email identification list, visually represented using a particular color that is associated with the particular detection mechanism, wherein the particular color is different from another color that is associated with another detection mechanism.

8. (Original) The system of claim 1, wherein the particular undesired email message is, within an email identification list, visually represented using a particular lettering style that is associated with the particular detection mechanism, wherein the particular lettering style is different from another lettering style that is associated with another detection mechanism.

9. (Currently Amended) A system for providing email service, comprising:

means for providing a plurality of detection mechanisms that detect undesired email messages at a user's computing device that receives the email messages from an email server;

means for designating an email message as being undesirable according to a particular detection scheme;

means for marking the email message at the user's computing device with a particular identifier of the particular detection scheme; and

means for displaying the email message at the user's computing device with the particular identifier in a particular visual manner that is associated with the particular identifier, wherein each of the detection mechanisms is represented using a different visual representation and the user's computing device upon detecting a drag and drop operation to move an email message from an inbox to a designated folder where the undesired email messages are stored prompts for the moved email message to be marked as a type of undesired email message that is associated with one of the detection mechanisms.

10. (Original) The system of claim 9, wherein the plurality of detection mechanisms includes a means for detecting of an email message from a sender that is not on a list of senders authorized by the user.

11. (Original) The system of claim 9, wherein the plurality of detection mechanisms includes a means for detecting an email message from a sender that is on a list of unauthorized senders.

12. (Original) The system of claim 9, wherein the plurality of detection mechanisms includes a means for detecting an email message that contains a textual content string that is on a list of unauthorized textual content strings.

13. (Original) The system of claim 9, wherein the plurality of detection mechanisms includes a means for detecting an email message that has content that matches a designated level of overall content of previous messages that were determined to be undesirable.

14. (Original) The system of claim 9, wherein the plurality of detection mechanisms includes:

means for detecting an email message from a sender that is not on a list of senders authorized by the user;

a means for detecting an email message from a sender that is on a list of unauthorized senders;

a means for detecting an email message that contains a textual content string that is on a list of unauthorized textual content strings; and

means for detecting an email message that has content that matches a designated level of overall content of previous messages that were determined to be undesirable.

15. (Currently Amended) A method for providing email service, comprising:

providing a plurality of detection approaches for detecting undesired email messages at a user's computing device that receives the email messages from an email server;

designating an email message as being undesirable according to a particular detection scheme;

marking the email message at the user's computing device with a particular identifier of the particular detection scheme; ~~and~~

displaying the email message at the user's computing device with the particular identifier in a particular visual manner that is associated with the particular identifier, wherein each of the detection mechanisms is represented using a different visual representation;

detecting a drag and drop operation to move an email message from an inbox to a designated folder where the undesired email messages are stored; and

in response to detecting the drag and drop operation, prompting for the moved email message to be marked as a type of undesired email message that is associated with one of the detection mechanisms.

16. (Original) The method of claim 15, wherein the plurality of detection approaches include an approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user.

17. (Original) The method of claim 15, wherein the plurality of detection approaches includes an approach that detects an email message if the sender of the email message is on a list of unauthorized senders.

18. (Original) The method of claim 15, wherein the plurality of detection approaches include an approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content strings.

19. (Original) The method of claim 15, wherein the plurality of detection approaches include an approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of previous messages.

20. (Previously Presented) The method of claim 15, wherein the plurality of detection approaches includes:

an approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user;

an approach that detects an email message if the sender of the email message is on a list of unauthorized senders;

an approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content strings; and

an approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of the previous messages according to a designated content score.

21. (Original) The method of claim 20, wherein the particular visual manner is a particular color that is associated with a first detection approach, wherein the particular color is different from another color that is associated with a second detection approach.

22. (Original) The method of claim 20, wherein the particular visual manner is a particular lettering style that is associated with a first detection approach, wherein the particular lettering style is different from another lettering style that is associated with a second detection approach.

23. (Previously Presented) The method of claim 15, further comprising:

recognizing which particular detection approach designated the email message as being undesirable upon the visual representation of the email message.